UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 16-CR-38

MARCUS A. OWENS,

Defendant.

UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS (Doc. #37)

The United States of America, by and through it attorneys, Gregory J. Haanstad, United States Attorney for the Eastern District of Wisconsin, and Benjamin W. Proctor, Assistant United States Attorney for this District, hereby responds in opposition to defendant Marcus Owens's "Motion to Suppress." Doc. #37.

I. Introduction

After a months-long investigation, the FBI briefly assumed administrative control of Playpen, a website dedicated to the sharing of child pornography. The FBI sought and obtained a warrant permitting it to deploy a "Network Investigative Technique" ("NIT") during that same period, which would cause a computer logging into Playpen to reveal certain identifying information—most importantly, its concealed Internet Protocol ("IP") address. Among the IP addresses identified accessing Playpen was one associated with Marcus Owens. Following the execution of a search warrant at Owens's home in

Kenosha, Wisconsin, Owens was indicted for receiving and possessing child pornography.

Owens now seeks to suppress the information obtained by the NIT and used to identify his home computer and its location, along with all other evidence derived from that information. He presents several arguments.[1] First, he asserts that the NIT warrant was not supported by probable cause. Second, he asserts that the NIT warrant affidavit included "recklessly misleading statements that justify a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978). Third, he contends that the NIT warrant was overbroad and lacked particularity. Fourth, he contends that the NIT warrant was an anticipatory warrant that lacked a triggering event. And fifth, Owens contends that the NIT warrant did not authorize a search of Owens's computer in Wisconsin.

Each of these arguments is meritless. In fact, as far as the United States can tell, each of arguments Owens presents in this motion to suppress has been rejected by the various federal courts that have previously considered them.[2] For instance, in *United States v. Epich*, Case No. 15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016), another branch of this Court rejected arguments that the NIT warrant was not supported by probable cause and that the NIT warrant lacked particularity. In *United States v. Michaud*, Case No. 15-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016), the district court in

[1] This is one of three motions filed by Owens on August 1, 2016. The other motions seek to suppress evidence based on the magistrate judge's lack of jurisdiction, Doc. #40, and to dismiss the indictment based on outrageous government conduct, Doc. #41. The United States is filing separate responses to all of the motions.

[2] Copies of district court decisions cited in this response and in the United States' response to Owens's related motion to suppress (Doc. #40) are attached to this filing.

the Western District of Washington rejected a defendant's arguments that the NIT warrant was an unconstitutional "general warrant"; that there was a material misrepresentation that justified a *Franks* hearing; and that deployment of NIT to defendant's computer in Washington State exceeded the scope of the warrant. In *United States v. Matish*, Case No. 2016 WL 3455776 (E.D. Vir. June 23, 2016), the district court for the Eastern District of Virginia rejected a defendant's arguments that the NIT warrant lacked probable cause; that there was a material misrepresentation that justified a *Franks* hearing; that the NIT warrant was overbroad and lacked particularity; and that the "triggering event" never occurred. In *United States v. Darby*, Case No. 16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016), the district court for the Eastern District of Virginia rejected a defendant's argument that the NIT warrant lacked probable cause; that there was a material misrepresentation that justified a *Franks* hearing; that the NIT warrant was overbroad and lacked particularity; and that the "triggering event" never occurred. Similarly, in *United States v. Eure*, Case No. 16-C-R43, 2016 WL 4059663 (E.D. Va. July 28, 2016), the district court for the Eastern District of Virginia addressed the exact same arguments presented *Darby* (and here), incorporated the *Darby* decision, and expanded on why suppression is not be appropriate under the circumstances. Of note, the district courts in *Matish* and *Michaud* held hearings in which government agents and defense experts testified regarding the NIT warrant materials. After hearing from the witnesses, those courts rejected all of those defendants' arguments.

II. Background

The charges in this case arise from an investigation into Playpen, a global online forum through which registered users (including Marcus Owens) advertised, distributed, and/or accessed illegal child pornography. The scale of child sexual exploitation on the site was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography. Images and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site also included forums for discussion for all things related to child sexual exploitation, including tips for grooming victims and avoiding detection.

A. Playpen users, including Marcus Owens, used the Tor network to access child pornography while avoiding law enforcement detection.

Playpen operated on the anonymous Tor network. Tor was created by the U.S. Naval Research Laboratory as a means of protecting government communications. It is now available to the public. The Tor network—and the anonymity it provides—is a powerful tool for those who wish to share ideas and information, particularly those living in places where freedom of speech is not accorded the legal protection it is here. But this anonymity has a downside. The Tor network is a haven for criminal activity in general, and for the online sexual exploitation of children in particular. *See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, Wired Magazine, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited August 8, 2016).

Use of the Tor network masks the user's actual Internet Protocol ("IP") address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers.[3] To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." Users can also access Tor through "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address, Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open Internet are not viable.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate the same as other public websites with one critical exception: namely, the IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and operating in the Tor network. And unlike an open Internet website, it is not possible to use public lookups to determine the IP address of a computer hosting a "hidden service."

[3] Additional information about Tor and how it works can be found at www.torproject.org.

A "hidden service" like Playpen is also more difficult for users to find. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find Playpen, a user had to first get the web address for it from another source—such as another Playpen user or online postings identifying Playpen's content and location. Accessing Playpen thus required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity occurring on Playpen, investigators faced a tremendous challenge when it came to identifying Playpen users. Because Tor conceals IP addresses, normal law enforcement tools for identifying Internet users would not work. So even if law enforcement managed to locate Playpen and its IP logs, traditional methods of identifying its users would have gone nowhere.

Acting on a tip from a foreign law enforcement agency as well as information from its own investigation, the FBI determined that the computer server that hosted Playpen was located at a web-hosting facility in the United States. In February 2015, FBI agents apprehended the administrator of Playpen and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of Playpen to go unidentified (and un-apprehended), the FBI allowed it to continue to operate at a government facility in the Eastern District of Virginia for the brief period from February 20, 2015, and March 4, 2015.

The FBI obtained court authorizations from the United States District Court for the Eastern District of Virginia to (1) monitor the site users' communications, and (2) deploy a Network Investigative Technique ("NIT") on the site (hereinafter referred to as the "NIT warrant"). These tools would be used to identify registered users who were anonymously engaging in the sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation. The NIT warrant affidavit explicitly stated that the FBI would be taking over Playpen and operating it from a server in the Eastern District of Virginia during the period of authorization. Def.'s Ex. B ¶ 30.[4]

Using the NIT, the FBI identified an IP address associated with Playpen user "tinderbittles" and traced it to Marcus Owens's residence in Kenosha, Wisconsin. "Tinderbittles" had been a registered user of Playpen since February 3, 2015—before the FBI seized the site—and was observed accessing and downloading child pornography from the site on February 25, February 26, and March 1, 2015. *See* Def.'s Ex. A ¶¶ 25-31. On February 1, 2016, FBI agents in the Eastern District of Wisconsin obtained a search warrant for Owens's home. Def.'s Ex. A. That warrant was executed on February 4, 2016. During the search, agents recovered computers and removable hard drives that contained more than 30,000 images and 3,000 videos of child pornography. Owens was arrested on February 10, 2016. Following his arrest, Owens stated to agents that he used

[4] Copies of the NIT search warrant, application, affidavit and return, were attached to the defendant's motion as Exhibit B. *See* Doc. #39-2. Copies of the search warrant, application, and affidavit for Owens residence were attached to the defendant's motion as Exhibit A. *See* Doc. #39-1.

the Tor network and accessed Playpen using the user name "tinderbittles." Owens admitted that he had been accessing child pornography for several years.[5] On March 1, 2016, the grand jury returned an indictment charging Owens with receipt and possession of child pornography. Doc. #1.[6]

B. Based on the nature of Playpen and the Tor network, law enforcement sought and obtained court approval to deploy a NIT to identify criminals engaged in the creation, advertisement, and distribution of child pornography.

The 31-page NIT search warrant affidavit was sworn to by a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. Def.'s Ex. B ¶ 1. The affidavit comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist law enforcement in identifying registered site users. Those users were using anonymizing technology to conceal online child sexual exploitation on a massive scale.

[5] Among other things, Owens admitted to having saved thousands of images and hundreds of videos. He said that he had been accessing child pornography since age 20 or 21 (he was 27 at the time of the interview).

[6] In his motion, Owens asserts that "Mr. Owens has never been previously charged with any criminal offense." Doc. #37 at 19. This is true. But Owens has been previously accused of sexually assaulting a child, and based on evidence recovered by the FBI during the search warrant executed in connection with this case, the State of Wisconsin charged Owens with First Degree Child Sexual Assault in violation of Wis. Stat. § 948.02(1)(e), in Kenosha County Case No. 2016CF0376. That case is pending, and Owens of course remains innocent until proven guilty.

1. The NIT warrant affidavit set forth in great detail the technical aspects of the investigation that justified law enforcement's request to use the NIT.

In recognition of the technical and legal complexity of the investigation, the NIT warrant affidavit included: a three-page explanation of the offenses under investigation, Def.'s Ex. B ¶ 4; a seven-page section setting out definitions of technical terms used in the affidavit, Def.'s Ex. B ¶ 5; and, a three-page explanation of the Tor network, how it works, and how users could find a hidden service such as Playpen, Def.'s Ex. B ¶¶ 7-10. The affidavit spelled out the numerous affirmative steps a user would have to go through just to find the site. Indeed, the agent explained:

> Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. [Playpen] is listed in that section.

Def.'s Ex. B ¶ 10. Thus, the agent continued, "[a]ccessing [Playpen] . . . requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." Def.'s Ex. B ¶ 10.

2. Playpen was dedicated to the advertisement and distribution of child pornography, a fact that would have been apparent to anyone who viewed the site.

The affidavit also described in great detail and in stark terms the purpose of Playpen and why its users were appropriate targets for the NIT. Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes." Def.'s Ex. B ¶ 6. More to the point, "administrators and users of [Playpen] regularly sen[t] and receive[d] illegal child pornography via the website." Def.'s Ex. B ¶ 6. The agent also addressed the sheer scale of the illicit activity occurring on Playpen: site statistics as of February 3, 2015, for Playpen—which was believed to have been in existence only since August of 2014—showed that it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.[7] Def.'s Ex. B ¶ 11.

Playpen's illicit purpose was also apparent to anyone who visited it during the six months it operated before the FBI seized control of it. "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." Def.'s Ex. B ¶ 12. And the following

[7] As the affidavit explained, a bulletin board website such as Playpen is a website that provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Def.'s Ex. B ¶ 5(a).

text appeared beneath those young girls: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." While those terms may have seemed insignificant to the untrained eye, the affiant explained, based on his training and his experience, that the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being 're-posted'" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." Def.'s Ex. B ¶ 12. The combination of sexualized images of young girls along with these terms of art referencing image posting and large file compression unmistakably marked Playpen as just what it was—a hub for the trafficking of illicit child pornography.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site and highlighted the emphasis the registration terms placed on users avowing being identified. Users clicking on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in the affidavit. Def.'s Ex. B ¶¶ 12-13. Playpen repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating, "the forum operators do NOT want you to enter a real [e-mail] address," users "should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing or Tor we also recomend [sic] that you turn off javascript and disable sending of the 'referer' header." Def.'s Ex. B ¶ 13. This

focus on anonymity is entirely consistent with the desire on the part of Playpen administrators and users to evade detection of their illicit activities.

Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail address. Def.'s Ex. B ¶ 14. Upon successful registration, all of the sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observable. Def.'s Ex. B ¶ 14. The vast majority of those sections and forums were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. For instance, within the site's "Chan" forum were individual sub-forums for "jailbait" or "preteen" images of boys and girls. Def.'s Ex. B ¶ 14. There were separate forums for "Jailbait videos" and "Jailbait Photos" featuring boys and girls. Def.'s Ex. B ¶ 14. The "Pre-teen Videos" and "Pre-teen Photos" forums were each divided into four sub-forums by gender and content, with "hardcore" and "softcore" images/videos separately categorized for Boys and Girls. Def.'s Ex. B ¶ 14. A "Webcams" forum was divided into Girls and Boys sub-forums. Def.'s Ex. B ¶ 14. The "Potpurri" forum contained sub-forums for incest and "Toddlers." Def.'s Ex. B ¶ 14.[8]

[8] Defendant attempts to characterize Playpen as something other than a child pornography forum. *See, e.g.*, Doc. #37 at 2 ("Playpen contained a mix of legal and illegal content . . . and did not advertise itself as a child pornography site."); Doc. #37 at 11 ("Playpen offered a mix of chat forums, private messaging services, both legal and illegal pictures and videos, and links to pictures and videos."). For instance, he notes that the page listing the sections, forums, and sub-forums did not itself contain images of child pornography, and that some of the names of the sections and forums are not necessarily indicative of child pornography. *See* Doc. #37 at 16-17. According to the defendant, only "some of these [listings] also clearly relate to children." Doc. #37 at 16. He cites sections listed as "artwork" and "stories" and "general discussion" which he contends could refer to innocent, legal activities. Doc. #37 at 16. These assertions are absurd. No rational person aware of the context would look at this listing and think it was not dedicated to child pornography. Indeed, the defendant fails to mention that the reference to "artwork" follows a listing for "toddlers" which follows a listing for "Family Playpen – Incest," which follows several listings for webcams of "boys" and

The affidavit also described, in graphic detail, particular child pornography that was available to all registered users of Playpen, including images of prepubescent children and even toddlers, being sexually abused by adults. Def.'s Ex. B ¶ 18. Although the affidavit clearly stated that "the entirety of [Playpen was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." Def.'s Ex. B ¶ 27.

The affidavit further explained that Playpen contained a private messaging feature that allowed users to send messages directly to one another. The affidavit specified that "numerous" site posts referenced private messages related to child pornography and exploitation, including an example where one user wrote to another, "I can help if you are a teen boy and want to fuck your little sister, write me a private message." Def.'s Ex. B ¶ 21. Based on the affiant's training and experience and law enforcement's review of the site, the affiant stated his belief that the site's private message function was being used to "communicate regarding the dissemination of child pornography." Def.'s Ex. B ¶ 22. The affidavit also noted that Playpen included multiple other features intended to facilitate the sharing of child pornography, including an image host, a file host, and a chat service. Def.'s Ex. B ¶¶ 23-25. All of those features allowed site users to upload, disseminate, and access child pornography. And the affidavit included detailed examples

"girls," which follow several listings for "pre-teen photos" of "girls HC" and "boys HC." *See* Def.'s Ex. B ¶ 14.

and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features. Def.'s Ex. B ¶¶ 23-25.

3. The NIT warrant affidavit and attachments explained what the NIT would do and precisely identified the seven pieces of information it would collect and send back to government-controlled computers.

The NIT warrant affidavit contained a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.[9]

Specifically, the affidavit noted that without the use of the NIT "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." Def.'s Ex. B ¶ 29. Further, because of the "unique nature of the Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed." Def.'s Ex. B ¶ 31. The affiant thus concluded, "using a NIT may help FBI agents locate the

[9] Owens repeatedly describes the NIT as "malware" in an apparent attempt to paint the technique as malign. *See* Doc. #37 at 1, 7, 12, 18, 39. That label is unhelpful to the Court's analysis. As discussed herein, the NIT is a legitimate law enforcement tool. Here, its use was judicially authorized based on a showing of probable cause. It consisted of computer instructions designed to cause the user's computer to transmit a limited set of information to assist in identifying the computer used to access Playpen and its user. Indeed, as one court observed in dismissing the defendant's characterization of the NIT as malware: "perhaps malware is a better description for the program through which the provider of the pornography attempted to conceal its distribution of contraband over the Internet than for the efforts of the Government to uncover the pornography." *Matish*, 2016 WL 3545776, at *9.

administrators and users" of Playpen. Def.'s Ex. B ¶¶ 31-32. Indeed, he explained, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. Def.'s Ex. B ¶ 31.

In terms of the deployment of the NIT, the affidavit explained that when a user's computer downloads site content in the normal course of operation, the NIT would augment that content with additional computer instructions. Def.'s Ex. B ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. Def.'s Ex. B ¶ 33. The discrete pieces of information to be collected were detailed in the NIT warrant and accompanying Attachment B, along with technical explanations of the terms. They were limited to the following: (1) the actual IP address assigned to the user's computer; (2) a unique identifier to distinguish the data from that collected from other computers; (3) the operating system running on the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's Host Name; (6) the computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. Def.'s Ex. B ¶ 34.

The affidavit explained exactly why the information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." Def.'s Ex. B ¶ 35. For instance:

> the actual IP address of a computer that accesses [Playpen] can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

Def.'s Ex. B ¶ 35.

The affidavit specifically requested authority to deploy the NIT each time any user logged into Playpen with a username and a password. Def.'s Ex. B ¶ 36. However, the affidavit disclosed to the magistrate that, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation," the FBI might "deploy the NIT more discretely against particular users," including those who "attained a higher status" on the site or "in particular areas of [Playpen]" such as the sub-forums with the most egregious activity, which were described elsewhere in the affidavit. Def.'s Ex. B ¶ 32 n.8. Finally, the affidavit requested authority for the NIT to "cause an activating computer—wherever located—to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." Def.'s Ex. B ¶ 46(a).[10]

[10] Owens's motion appears to mischaracterize the language of Attachment A. He implies that Attachment A listed the place to be searched as the "Target Website" and that the "activating computers" were "an additional place to be searched." *See* Doc. #37 at 18. In truth, Attachment A states at the outset "This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below." Def.'s Ex. B Att. A. Attachment A then defines the "target website," including its location

4. Hours before the NIT warrant was signed, Playpen's administrator changed the site logo, replacing two sexually suggestive images of a prepubescent girl with one sexually suggestive image of a prepubescent girl.

As noted above, among the things described in the NIT warrant affidavit was Playpen's site logo: "on the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent females with their legs spread apart." Def.'s Ex. B ¶ 12. A screenshot showing this logo as of February 3, 2015, was provided to the defense in discovery, and it is attached to the Defendant's motion as Defendant's Exhibit F. Between September 16, 2014 and February 3, 2015, FBI agents reviewed Playpen in an undercover capacity to document the activity on the site. Def.'s Ex. B ¶ 11. Sometime before February 18, 2015, Playpen's administrator changed the URL—the site address. Noticing that the URL had changed, the affiant visited Playpen on February 18, 2015, and confirmed that the content had not changed. Def.'s Ex. B ¶ 11 n.3. This includes the site logo.

In the evening of February 19, 2015, the FBI executed a search at the Florida home of the Playpen administrator and apprehended him. Def.'s Ex. B ¶ 30. At that point, the FBI also assumed control of Playpen. Postings by the administrator from earlier in the day show that just before he was arrested, the administrator changed Playpen's site logo, replacing the images described above with a single image showing a prepubescent girl,

in the Eastern District of Virginia, and defines the "activating computers" as those of any user or administrator who logs into the target website by entering a username and password. Def.'s Ex. B Att. A.

wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. A screenshot of this altered logo was provided to the defense in discovery and is attached to the Defendant's motion as Defendant's Exhibit C. The text described in the affidavit as part of the logo, "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview," which the affidavit explained pertain to image distribution, remained unchanged. *Compare* Def.'s Ex. B ¶ 12 *and* Def.'s Ex. F with Def.'s Ex. C. The NIT warrant was sworn to and authorized at 11:45 a.m. on February 20, 2015, the day after the logo change. The affidavit did not reference this recent change.

III. Argument

A veteran FBI agent with nearly two decades of experience explained to a neutral and detached magistrate why there was probable cause to believe that registered users of Playpen (1) knew Playpen was a website dedicated to the sexual exploitation of children, and (2) intended to use Playpen for its express purposes—viewing and sharing child pornography. He supported this conclusion with a detailed description of the steps required to find Playpen and register as a user, and the numerous indicators of Playpen's illicit purpose. That purpose was obvious to even a casual observer; however, the agent also was able to relate his considerable training and experience and determine that the likelihood that any user of Playpen was ignorant of the fact that it was a forum dedicated to child pornography was exceedingly low.

Relying on this information, the magistrate judge authorized the FBI to deploy a NIT to gather a limited set of identifying information from any user who logged into Playpen while it operated under FBI control. The warrant included a clear description of

which computers would be searched—any computers that logged into Playpen—and seven pieces of information that would be seized. The Fourth Amendment requires no more.

As detailed below, nothing in Owens's Motion to Suppress undermines this conclusion. The defects he identifies, if they are even considered defects, are neither of constitutional magnitude nor the result of an intention on the part of the FBI to mislead the magistrate or skirt the rules. Owens's contrary assertions find no support in the record. Defendants seeking the extraordinary remedy of suppression must clear a high hurdle. Owens falls far short, and his motion should therefore be denied.

A. As another branch of this Court has previously determined, the NIT warrant affidavit amply supports the magistrate judge's finding of probable cause for issuance of the NIT warrant.

Owens first contends that "the NIT warrant was not supported by probable cause." Doc. #37 at 19. For support, Owens asserts that it was not clear that Playpen was actually a child pornography site because "only facts that would support the conclusion that the site was clearly dedicated to child pornography are the description of two pictures that appear on the site's banner . . . 'depicting partially clothed prepubescent females with their legs spread apart,'" Doc. #37 at 20-21; and that the word "Playpen" can mean various things, Doc. #37 at 23-24. Relatedly, he asserts that the NIT warrant "did nothing to distinguish between 'accidental browsers'" and those who actively sought child pornography. *See* Doc. #37 at 19-28.[11]

[11] Elsewhere in the motion, Owens contends that the representations in the NIT warrant application were false. Those contentions are erroneous and are addressed next. However, for purposes of this aspect of his

Owens's arguments are meritless for several reasons. For instance, Owens's contention that the illicit purpose of Playpen was not "readily apparent" (despite images of partially clothed prepubescent girls, the unique registration terms and warnings, the graphic content listing upon registration, etc.) is nothing more than a self-serving, skewed interpretation of affidavit. And, the affiant's description of the main page was only one of many factors contributing to the probable cause determination. Among other things, the affidavit explained the unique nature of the Playpen site on the Tor network and the numerous affirmative steps required to access the site. Moreover, Owens's arguments regarding the "accidental browser" fall flat because, for the myriad reasons described in the affidavit, access by an accidental browser was extremely unlikely. In all, the affiant set forth specific, articulable facts that, along with interferences drawn from his training and experience, established probable cause to believe that registered users who logged into Playpen did so intending to view and trade child pornography. *See generally, e.g., Illinois v. Gates*, 462 U.S. 213, 238 (1983) (discussing probable cause standard); *United States v. Pritchard,* 745 F.2d 1112, 1120 (7th Cir. 1984) (discussing standard of review on challenge to magistrate judge's finding of probable cause); *United States v. Elst*, 579 F.3d 740, 746 (7th Cir. 2009) ("Experienced law enforcement officers (as well as experienced magistrates) are permitted to draw reasonable inferences from the facts based on their training and experience.").

motion, Owens asserts that even assuming everything in the affidavit is accurate, it still failed to establish probable cause.

Most importantly, however, another branch of this Court has *already considered and rejected* the arguments Owens now presents. In *United States v. Epich*, No. 15-CR-163, a related case stemming from the same NIT warrant, the defendant moved the Court to suppress evidence because the NIT warrant failed to establish probable cause. Like Owens, Epich asserted, among other things, that "although the affidavit states that this log in page contains images of two girls, the log in page says nothing about child pornography or any explanation whatsoever of what might be inside the site." *See* Epich's Mot. to Suppress at 13 ("Epich Mot."); Epich Reply Br. in Support of Mot. to Suppress at 11 ("Epich Reply") (asserting that "[t]he only basis to search the computer of every person who accessed [the site] would be if its pre-log-on pages showed that the site contained illegal pornography. But they did not."). This is substantively indistinguishable from Owens's claim that the affiant's description of the log-in page does not establish probable cause. Similarly, Epich argued that individuals could access the website "quite easily" and not view child pornography, and therefore the warrant was "overbroad and probable cause was lacking." Epich Mot. at 15; Epich Reply at 14. This is substantively indistinguishable from Owens's claim that the warrant did not distinguish between "accidental browsers" and individuals seeking child pornography.

Upon consideration of the parties' arguments along with the legal standard for probable cause, Magistrate Judge Jones issued a Report and Recommendation ("Epich Rec.") that Epich's motion be denied. District Judge Pepper adopted the Recommendation and denied the motion. *See* Decision and Order Adopting Magistrate Judge's Report and Recommendation and Denying Defendant's Motion to Suppress,

United States v. Epich, Case No. 14-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016). In the Recommendation (*Epich* Rec.), the Court discussed in detail the grounds supporting the issuing magistrate judge's probable cause finding. [12] *Epich* Rec. 13. The Court then walked through the affidavit and the arguments, finding that "it is highly unlikely that the NIT Warrant subjected to search users who stumbled upon the website by pure happenstance because users had to engage in numerous affirmative steps just to gain access to the site's content." *Id.* at 13-14. As noted by the Court, "by describing the nature of the website and the steps required to find it, the affidavit supported the reasonable inference that users likely discovered the web address via other forums dedicated to child pornography." *Id*. at 14.

The Court also commented on the affidavit's description of the main page. *Id.* at 14-15. It concluded that "the juxtaposition of the suggestive images and the text referencing terms associated with sharing images and/or videos created a strong inference that the site contained child pornography." *Id.* at 15. The Court considered and rejected the arguments that the presence of legal material on the site, and the affidavit's failure to differentiate users negated probable cause. *Id.* at 16-17. Looking to the "totality of the circumstances," the Court found that the facts described in the affidavit "created a reasonable inference that registered users who accessed the website knew that it

[12] It appears from the docket in *Epich* that Magistrate Judge Jones's Recommendation, Doc. #53, remains under seal. As discussed herein, the United States relies on the reasoning set forth in the Recommendation as part of its response in this case. However, rather than seeking permission to file a copy of this Court's own Recommendation under seal as part of this response, the United States presumes the Court has access to that document.

contained child pornography and accessed the site with the intent to view this illicit material. Accordingly, the issuing magistrate judge had a substantial basis for concluding that probable cause existed to issue the NIT Warrant." *Id.* at 16.

Nothing of legal or factual significance has changed since the Court issued its Recommendation and Order in *Epich*, and Owens provides no argument otherwise.[13] In fact, Owens offers no analysis of the *Epich* Order, or the various other district court decisions that have all rejected similar challenges to the magistrate judge's probable cause finding. *See e.g., Matish*, 2016 WL 3545776, at *9-11 (addressing similar arguments, citing *Epich* and other cases, and concluding that "the magistrate judge possessed ample probable cause to issue the NIT Warrant"); *Darby*, 2016 WL 3189703, at *7-8 ("In sum, the information in the affidavit provided substantial evidence in support of the magistrate's finding that there was probable cause to issue the NIT Warrant.").

B. Owens has made no showing that justifies a *Franks* hearing, let alone established that the NIT warrant affidavit contained a material and intentional or reckless falsehood or omission.

Owens next contends that the NIT warrant application contains "recklessly misleading statements and omissions." Doc. #37 at 28. In particular, Owens contends that the affiant "knowingly misportrayed the website's homepage," and that the affiant was not truthful when discussing how Playpen could be found. He therefore requests a hearing under the standard set forth in *Franks v. Delaware*, 438 U.S. 154 (1978).

[13] Owens's comparison of this case to *United States v. Gourd,* 440 F.3d 1003 (9th Cir. 2006) and *United States v. Shields*, 458 F.3d 269, 280 (3d Cir. 2006) add nothing. In fact, the *Epich* Recommendation cited to both *Gourd* and *Shields*. *Epich* Rec. at 17.

In order for Owens to be entitled to a *Franks* hearing, he "must make a 'substantial preliminary showing' that: (1) the affidavit contained a material false statement; (2) the affiant made the false statement intentionally, or with reckless disregard for the truth; and (3) the false statement was necessary to support the finding of probable cause." *See United States v. Maro*, 272 F.3d 817, 821 (7th Cir. 2001) (quoting *Franks*, 438 U.S. at 155-56). Allegations that the affidavit omitted material statements are subject to the same standard. *See United States v. Williams*, 737 F.2d 594, 604 (7th Cir. 1984).

The burden on the movant in seeking a *Franks* hearing is "substantial." *United States v. Johnson*, 580 F.3d 666, 670 (7th Cir. 2009). "[A]ffidavits supporting a search warrant are presumed valid, and . . . the 'substantial preliminary showing' that must be made to entitle the defendant to an evidentiary hearing must focus on the state of mind of the warrant affiant, that is the police officer who sought the search warrant." *United States v. Jones*, 208 F.3d 603, 607 (7th Cir. 2000) (citing *Franks*, 438 U.S. at 171). "The defendant must offer evidence showing either that the warrant affiant lied or that the warrant affiant recklessly disregarded the truth because he 'in fact entertained serious doubts as to the truth of his allegations' or had 'obvious reasons to doubt the veracity of the allegations.'" *Id.* (citing *Williams*, 737 F.2d at 602). Negligence by the affiant does not constitute reckless disregard for the truth. *See United States v. A Residence Located at 218 Third Street*, 805 F.2d 256, 258 (7th Cir. 1986). With this in mind, "*Franks* hearings are rarely required." *Johnson*, 580 F.3d at 670 (citing *Maro*, 272 F.3d at 821).

1. Owens's exaggerations regarding the home page are meritless.

Owens's primary beef is that the NIT warrant affidavit's description of the main page was not accurate. Doc. #37 at 31. The basis for this assertion is that up until February 19, 2015, the main page included "two images depicting partially clothed prepubescent girls" on either side of the site name. This was the description in the NIT warrant affidavit. Def.'s Ex. B ¶ 12. However, on February 19, 2015, a few hours before his arrest, the website administrator changed the main page so that instead of depicting two partially clothed prepubescent girls, it depicted one provocatively-dressed prepubescent girl. *See* Def.'s Ex. A at ¶ 12 & n.5 (noting that "On February 19, 2015, the site administrator replaced those two images with a single image, located to the left of the site name, depicting a prepubescent female, wearing a short dress and black stockings, posed sitting reclined on a chair with her legs crossed, in a sexually suggestive manner, and the text 'No cross-board reposts, .7z preferred, Encrypt filenames, Include preview,' to the right of the image."); Def.'s Exs. C & F. According to Owens, probable cause rested on the accurate description of these images, and that by "including an incorrect description of the site," a *Franks* hearing is warranted. Doc. #37 at 30.

Owens is wrong for several reasons. First, there is no evidence that any omission of the administrator's change to the Playpen logo just before the NIT warrant was authorized was reckless, let alone intentional. Indeed, the affiant had checked Playpen on February 18, 2015, the day before the logo changed, and the description was accurate at that time. Def.'s Ex. B ¶¶ 11-12 & n.3. The most that can be said is that, with the benefit of hindsight, it would have been better for the affiant to have reviewed Playpen again the

morning the warrant was signed, as opposed to two days before. If this is a failing at all, which is by no means obvious, it was—at worst—an unintentional oversight of an immaterial matter. *See, e.g., Darby*, 2016 WL 3189703, at *9 ("There is nothing reckless about relying on a visit to the website on February 18, 2015 when describing the website for a warrant signed and executed on February 20, 2015."); *Matish*, 2016 WL 3545776, at *12 ("The Court also finds that it was not reckless for the affiant not to examine the website one more time on the day he sought the warrant's authorization, as he had recently examined the website and confirmed that nothing had changed.").[14] Even if characterized as negligence (which it should not be), that is insufficient to justify a *Franks* hearing. *See, e.g., United States v. Prideaux-Wentz*, 543 F.3d 954, 962 (7th Cir. 2008) (noting that negligence is insufficient to justify a *Franks* hearing) (citing *United States v. Swanson*, 210 F.3d 788, 791 (7th Cir. 2000)).

Moreover, even assuming that failing to include a sentence referencing the changed image was somehow intentional and reckless (though it was not), the image change was utterly immaterial to the finding of probable cause. As noted, the images of two partially clothed prepubescent girls with their legs open were on the website up until February 19, 2015. The replacement of those two sexually-suggestive images of prepubescent girls with one sexually-suggestive image of a prepubescent girl the day before the warrant was issued in no way calls into question the illicit nature of the

[14] The district court in *Matish* took testimony from government agents on this point. Upon consideration of the testimony, which was subject to cross examination, the court found no support for the defendant's position. *See Matish*, 2016 WL 3545776, at *4, 12-13.

website. The relevance of the image(s) in the Playpen logo was that it/they sexualized young girls. That was true before February 19, 2015, and it remained true after. *See e.g.*, *Darby*, 2016 WL 3189703, at *7 ("To the extent one can or should differentiate among sexualized depictions of children, the images of the two girls that were previously on the homepage are more reprehensible. But that distinction does not subtract from the sexualized nature of the single image of child erotica that appeared on the homepage during the period in which the government operated Playpen. Either version of the homepage supports a finding of probable cause."); *Matish*, 2016 WL 3545776, at 12 (finding that "the logo change was not material to the probable cause determination" and citing testimony); *Michaud*, 2016 WL 337263 at *1 n.1 (noting court's oral denial of defendant's motion requesting *Franks* hearing). On top of this, as detailed above, the magistrate judge's probable cause finding rested on a host of facts and inferences that demonstrated a "fair probability" that anyone who logged into Playpen did so intending to view and/or share child pornography. *See Gates*, 462 U.S. at 238–39 (noting that "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place); *see also Darby*, 2016 WL 3189703, at *9 ("As discussed, contrary to the repeated emphasis of Defendant, the images of two prepubescent females described in the warrant application were not necessary to the finding of probable cause. There was an abundance of other evidence before the magistrate judge that supported her finding that there was probable cause to issue the warrant.").

Owens other criticisms of the home-page description fall far short of warranting a *Franks* hearing. For instance, Owens faults the agent for not "mention[ing] how small the [image of prepubescent girls on the home page] is." Doc. #37 at 31. According to Owens, the image is "so small that one has difficulty making out the details" and that it is "tucked away in a corner, not a prominent feature of the home page." These are simply self-serving (and inaccurate) opinions. The same goes for his assertion that affiant did not reference the "chat forum" which is "prominent" on the home page. This is simply a criticism of content decisions by the affiant, not a valid allegation that the affidavit is intentionally or recklessly misleading. Moreover, the affidavit did discuss the chat feature. *See* Def.'s Ex. B ¶¶ 23-25. In fact, it provided specific examples of Playpen's chat feature being used for the purpose of distributing child pornography. Def.'s Ex. B ¶ 25.

2. Owens mischaracterizes the affidavit in his effort to obtain a *Franks* hearing.

Owens also asserts that "the affidavit misleadingly describes how difficult it is to find websites on the Tor network, going so far as to suggest there is no such thing as a Tor equivalent of a Google search engine." Doc. #37 at 33. But this assertion is based on misrepresentations of the affidavit's contents. First, Owens wholly ignores that the paragraph at issue is focused Tor "hidden services." Def.'s Ex. B ¶ 10. There is no inaccuracy in the affiant's statements that a user must know "the web address of the website in order to access the site" and that "hidden services are not indexed like websites on the traditional internet." Def.'s Ex. B ¶ 10. Thus, this argument provides no grounds for a *Franks* hearing. Relatedly, Owens's contention that Tor search engines such as

"ahmia.fi" "may very well" lead people to searching for legal content to Playpen are pure, unsupported speculation. Such speculation does nothing to undermine the conclusions of a veteran FBI agent relying on his experience and that of other experts. Importantly, as noted in Defendant's Exhibit H, "ahmia.fi" apparently has a content-filtering policy that would remove pages containing child abuse (for which Playpen would certainly qualify). Defendant fails to address this point.[15] Even if it were otherwise, this would not call into question the reasonable conclusion that a user who managed to find Playpen and enter the site was aware of its purpose and content.[16]

Owens's assertion that "the affidavit misleadingly suggests that the government had looked for Playpen using conventional means" is also meritless. It is founded on the false premise (discussed above) that traditional search engines will reveal Playpen. Again, there is no dispute that Tor hidden services, such as Playpen, are not indexed like websites on the traditional internet. Def.'s Ex. B ¶ 10. Instead, "a user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location." Def.'s Ex. B ¶ 10. And the affidavit even listed an example of this, stating that

[15] Elsewhere in his brief, Owens's asserts that the "due to a misconfiguration, Playpen was intermittently accessible to regular internet users." Doc. #37 at 15. This is generally true, as explained in the NIT warrant affidavit, Def.'s Ex. B ¶¶ 28-29 & n.7, and the Owens residential warrant affidavit, Def.'s Ex. A ¶ 8 n.4. But the fact remains that "[i]n order to access [Playpen] in that manner, however, a user would have to had know[n] the exact IP address of the computer server that hosted [Playpen], which was not publically available." Def.'s Ex. A ¶ 8 n.4. To the extent Owens's is attempting to imply that Playpen was somehow available through a traditional search engine, that argument has no support.

[16] Indeed, at the end of it all, the affiant's conclusion, based on the facts and his training and experience, was that it was "extremely unlikely" for a user to have accessed Playpen without intent to view child; not impossible. The magistrate judge agreed.

there is a Tor "hidden service" page dedicated to pedophilia and child pornography that contained a section with links to Tor hidden services that contain child pornography, including Playpen. Def.'s Ex. B ¶ 10. Owens's contention that there are no "screenshots" of this website has no bearing on the accuracy or materiality of the affidavit.

Of note, the district court in *Darby* addressed and rejected a similar argument:[17]

> The warrant application asserts that, because sites on the Tor network are not searchable with the same ease that sites on the traditional internet are, most visitors to Playpen must have been told of site's online address and knew of the content of the site before registering. Defendant refutes this and identifies both a search engine and index of sites on the Tor network. Defendant claims that one could find Playpen when searching for sites containing sexually explicit content that was not child pornography. The government counters by noting that the search engine identified by Defendant filters out sites containing child abuse. Additionally, the warrant application notes that the address for Playpen was listed in a directory contain on another Tor hidden service that was dedicated to child pornography.
>
> Ultimately, no matter how searchable the Tor network may be, the magistrate judge would have been justified in concluding that those individuals who registered and logged into Playpen had knowledge of its illegal content. The Tor network itself, although it has legitimate uses, is an obvious refuge for those in search of illegal material. At the very least, the Tor network is less searchable than the regular Internet. Defendant fails to explain why someone would go to the trouble of entering the Tor network, locating Playpen, registering for the site, and then logging into the site if they were not looking for illegal content. It is not as if the Internet is not saturated in legal pornography. The magistrate's common sense judgment would justify her finding that an individual would likely only take these steps if he was

[17] This aspect of the *Darby* decision focused on the probable cause finding. Its conclusion, however, is certainly relevant to the *Franks* analysis, which requires a showing that that the alleged misrepresentation is material to the finding of probable cause. *See Maro*, 272 F.3d at 821.

> seeking child pornography and knew he could find it on Playpen.

Darby, 2016 WL 3189703, at *8. As in *Darby*, there are no grounds for concluding that the affidavit included a material misrepresentation or omission.

3. Owens's remaining arguments in support of a *Franks* hearing are off base or mere disagreements with the affiant's description.

Owens also takes issue with the affidavit's statement that "the entirety of [Playpen] is dedicated to child pornography." Doc. #37 at 35 (citing Def.'s Ex. B ¶ 27). To support this argument, Owens contends that such a description is undercut by "the table of contents." Owens also faults the affidavit for not "detail[ing] what specific sub-forums contained child pornography and what do not," noting that categories such as "general discussion" would appear not to contain such materials." Doc. #37 at 36. Finally, Owens contends that certain statements in the affidavit, while true, are "calculated to mislead." Doc. #37 at 36-37. All of these arguments are meritless.

First, Owens assertions are misleading. The table of contents, as detailed in paragraphs 14 and 27 of the affidavit, explicitly references "jailbait-boy," "jailbait-girl," "preteen-boy," "preteen-girl," "preteen videos" including "girls HC" and "boys HC," "toddlers," etc. And, the affiant stated that he had reviewed sub-forums, and that he had listed those that contained "the most egregious examples of child pornography and/or dedicated to retellings of real world hands on sexual abuse." Def.'s Ex. B ¶ 27; *see also* Def.'s Ex. B ¶ 16 (describing review of topics within the various forums). Indeed, the affiant does a thorough job of explaining the content of the site, none of which is alleged to be inaccurate. *See generally*, Def.'s Ex. B ¶¶ 14-18, 20-27.

The affidavit also addresses and undercuts Owens's assertion that forums such as "General Discussion" appear unconcerned about child pornography. In fact, the affidavit expressly states that a review of the "information and rules" topics, including the "General Discussion" topic, "revealed the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users." Def.'s Ex. B ¶ 17. Again, this is a site focused on sharing child pornography.

Finally, Owens's assertion that the affiant's discussion of website features is "calculated to mislead" is wrong. Specifically, Owens takes issue with paragraph 23, which describes the "Image hosting" feature as "allow[ing] users of [Playpen] to upload links of child pornography that are accessible to all registered users." Def.'s Ex. B ¶ 23. According to Owens, such "upload capabilities described by the affiant are basic features of many websites." Doc. #37 at 36. But this argument is pointless. While these capabilities may be basic feature of other websites, here they are used for sexually exploiting children. The affiant even describes his review of posts on that feature that linked to child pornography. Def.'s Ex. B ¶ 23.

In sum, nothing asserted by Owens comes close to calling into question the affiant's overarching statement that Playpen was dedicated to child pornography. At most, Owens quibbles with the affiant's description of the facts or the inferences to be drawn from those facts. But there are no falsehoods, let alone any falsehoods material to the finding of probable cause. Owens has therefore failed to make the substantial showing necessary to justify a *Franks* hearing.

C. The NIT warrant particularly described the locations to be searched and the things to be seized based on a showing of probable cause as to each.

Owens contends that the NIT warrant was overbroad and lacked particularity. Doc. #37 at 38-43. But the NIT warrant described specifically the places to be searched—activating computers of users or administrators that logged into Playpen—and the things to be seized—the seven pieces of information obtained from those activating computers. And a neutral and detached judge found that there was probable cause to support the requested search. The Fourth Amendment requires no more. Accordingly, the Court should decline Owens's invitation to read into the Fourth Amendment a heretofore undiscovered upper bound on the number of searches permitted by a showing of probable cause.

The constitutional principles at play here are well-settled. "[N]o warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV. The Constitution demands that two things be described with particularity: "'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006).

As to the place, "[t]he basic requirement is that the officers who are commanded to search be able from the 'particular' description of the search warrant to identify the specific place for which there is probable cause to believe that a crime is being committed." *United States v. White*, 416 F.3d 634, 637 (7th Cir. 2005) (citing *United States v. Hinton*, 219 F.2d 324, 326 (7th Cir. 1955)). As to the items to be seized, nothing must be "left to the discretion of the officer executing the warrant" in deciding what to seize.

Marron v. United States, 275 U.S. 192, 196 (1927). Whether this particularity standard is met is determined in light of the information available at the time the warrant issued. *White*, 416 F.3d at 637–38 (citing *Maryland v. Garrison*, 480 U.S. 79, 85 (1987)).

The NIT warrant meets both requirements. Attachments A and B of the NIT warrant, respectively, identified the "Place to be Searched" and the "Information to be Seized." Both defined with precision where agents could look and for what. The warrant authorized deployment of the NIT to the computer server hosting Playpen and then to computers of "any user or administrator who logs into [Playpen] by entering a username and password." Def.'s Ex. B, Att. A. Attachment B, in turn, imposed precise limits on what information could be obtained from those computers by the NIT: the seven pieces of information listed. Def.'s Ex. B, Att. B.

Indeed, another branch of this Court previously considered and rejected a challenge that the NIT warrant lacked particularity. In *Epich*, the Court found that "the NIT Warrant satisfied the Fourth Amendment's particularity requirement as it specifically described the place to be searched and the things to be seized." *Epich* Rec. 19-20. Other courts have reached the same conclusion. *See Matish*, 2016 WL 3545776, at *14 ("The Court finds that the NIT Warrant did not violate the Fourth Amendment's particularity requirement. The Court also finds that the warrant was not broader than the probable cause upon which it was based."); *Michaud*, 2016 WL 337263, at *5 ("Both the particularity and breadth of the NIT Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a general warrant."). This Court should reject Owens's attacks. *See* Doc. #37 at 42-43.

Sidestepping *Epich* (which goes unmentioned in his motion), Owens appears to cloak a separate argument under the guise of particularity and overbreadth challenge. In particular, he appears to press a novel constitutional rule for the Internet age: the NIT warrant is an unconstitutional "general warrant" because it authorized, upon finding of probable cause, the collection of specific information from a potentially large number of computers. Doc. #37 at 38-42. But, as discussed, the Fourth Amendment contains no such no such upper bound on the number of search locations a showing of probable cause can support.

The Fourth Amendment demands that there be probable cause to search a particular location for particular items. But the notion that a warrant supported by sufficient probable cause to authorize a search of numerous locations is, for that reason alone, constitutionally defective is wrong. Either probable cause exists to support a search or searches or it does not. Here, Owens maintains that the NIT warrant, which permitted the collection of information from any user or administrator who logged into Playpen, was not supported by sufficient facts to justify the search. Doc. #37 at 39. As explained above, however, he is incorrect. There was a fair probability that anyone who logged into Playpen did so with knowledge of its content and the intent to consume it. Accordingly, the warrant properly authorized the deployment of the NIT to any such user, regardless of how many there are or could be. *See Epich* Rec. 20; *see also Darby*, 2016 WL 3189703, at *8 ("Comparing this warrant to those outrages [of general warrants] trivializes the struggles of the American Revolution and the achievements of the Constitution. The NIT

Warrant describes particular places to be searched—computers that have logged into Playpen—for which there was probable cause to search. It is not a general warrant.");

Owens also contends that since the affidavit informed the magistrate judge that the FBI might deploy the NIT in a more targeted fashion to certain users—e.g., those users who accessed parts of Playpen containing the most egregious examples of child pornography—in order to ensure technical feasibility and avoid detection, Def.'s Ex. B ¶ 32 n.8, the FBI was somehow constitutionally compelled to do so. *See* Doc. #37 at 39-40. Owens is wrong. A warrant is "facially deficient" only when it fails to provide any meaningful instruction to the searching agents regarding the items to be seized. *See generally Marron*, 275 U.S. at 196. That the FBI retained discretion to execute the warrant on a narrower set of users does not somehow convert it into an unconstitutional general warrant.

Owens's reliance on Ninth Circuit decisions such as *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) is also misplaced. While the Ninth Circuit has cautioned its magistrate judges to be vigilant in approving electronic searches to strike "the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures," the NIT warrant hardly can be described as the sort of "general exploratory" search over which the Ninth Circuit has expressed concern. The limited scope of the NIT warrant's authorized search is certainly relevant in assessing its reasonableness and the magistrate judge's determination. The NIT warrant did not subject the defendant to a wholesale search of his electronic devices. Rather, the NIT collected seven pieces of

information that would assist law enforcement in identifying those suspected of trading and viewing child pornography.

Indeed, the most critical piece of information obtained by the NIT warrant—the defendant's IP address—is information that ordinarily would have been publicly available and therefore the defendant cannot claim a reasonable expectation of privacy. *See e.g., United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers"); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [Internet Service Providers]."); *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007).

Several courts have found that this principle applies in the context of Tor and NITs. *See e.g., United States v. Laurita*, Case No. 13-CR-107, 2016 WL 4179365, at *5 (D. Neb. Aug. 5, 2016) ("Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address."); *Matish*, 2016 WL 3545776, at *20 ("Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address."); *United States v. Werdene*, Case No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); ("Werdene had no reasonable expectation of privacy in his IP address. Aside from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party: 'in order for

a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations.'") (citing *United States v. Farrell*, Case No. 15-CR-029, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016)); *Michaud*, 2016 WL 337263, at *7 ("Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location.") (citing *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)).

In short, Owens's argument cannot defeat a validly obtained warrant, supported by probable cause, that particularly describes where to search and for what. That a warrant authorizes the search of a potentially large number of suspects is an indication, not of constitutional infirmity, but a large number of criminal suspects.

D. None of Owens's other claimed defects in the NIT warrant justify the extraordinary remedy of suppression.

None of the remaining flaws in the NIT warrant Owens identifies justify the extraordinary remedy of suppression. First, Owens claim that the NIT warrant was void because, as an anticipatory warrant, the "triggered event" never occurred is little more than a rehash of same probable cause and *Franks* challenges that have already been addressed. Next, his claim that the NIT warrant did not authorize deployment of the NIT to his computer because it was located in Wisconsin relies on an obtuse and crabbed reading of the authorizing warrant and its attachments that this Court should not

endorse. The FBI sought authority to deploy the NIT to activating computers, wherever located, and that is exactly what it did.

1. The NIT warrant was a valid anticipatory warrant.

Although Owens does not appear to challenge the notion that the NIT warrant could be categorized as an anticipatory warrant, he wrongly asserts that it was void because the "triggering event" that would authorize its execution against him never occurred. Doc. #37 at 43-44.

It is well-settled that the Fourth Amendment is no bar to "anticipatory warrants." These warrants are "no different in principle from ordinary warrants." *Grubbs*, 547 U.S. at 96. "[T]wo prerequisites of probability must be satisfied. It must be true not only that if the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place,' but also that there is probable cause to believe the triggering condition will occur." *Id.* at 96-97.

Here, contrary to Owens's assertions, the relevant "triggering event" was a user entering his username and password into Playpen and entering the site. And here too, the NIT warrant affidavit provided ample support for the probable cause determination as to both. Attachments A and B, which were incorporated into the warrant, specified the exact conditions under which the NIT was authorized to be deployed—i.e., when a user such as Owens logged into Playpen—and as discussed in detail above, there was probable cause to believe that any user who logged onto Playpen was seeking child pornography.

Owens posits that because this "triggering event" never occurred, the NIT warrant was void. Notably, he is not claiming that Owens did not in fact log into Playpen. Instead, Owens's argument on this point is just a reiteration of his probable cause and *Franks* challenges. As noted above, there was ample support for the magistrate's finding of probable cause, and Owens fails in his effort to make out a *Franks* challenge to the warrant. Accordingly, his claim about the absence of a "triggering event" to support execution the NIT warrant must also fail. Courts that have previously addressed this exact argument have rejected it. *See Matish*, 2016 WL 3545776, at *15 (finding that while the defendant's argument that the triggering event never occurred was "novel," "logging into Playpen represents the relevant triggering event" and that the triggering event did occur"); *Darby*, 2016 WL 3189703, at *9 (rejecting challenge, noting that "[l]ogging into Playpen was the triggering event, and all the computers searched under the NIT Warrant, including Defendant's, logged into the site."); *Eure*, 2016 WL 4059663, at *7 (noting defendant's characterization of the triggering event as logging into the site as it was exactly described in the application is a misrepresentation that attempts to transform an alleged problem in the application for the warrant into a problem in the execution of the warrant).

2. The NIT warrant plainly authorized deployment of the NIT to Owens's computer.

The NIT warrant, read in full, plainly authorized the deployment of the NIT to Owens's computer, notwithstanding the fact that it was physically located in Wisconsin. The warrant and accompanying attachments made clear to the magistrate judge that the

NIT was to be deployed initially to the web server hosting Playpen in the Eastern District of Virginia and that it was then to obtain information from computers that logged into Playpen, wherever they may be located.

No one, including the authorizing magistrate judge, could have thought otherwise. For starters, the warrant application and warrant are captioned "in the matter of the search of computers that access [the URL of Playpen]." Moreover, Attachment A to the warrant provided:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia. The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.

Def.'s Ex. B Att. A.

The affidavit also left no room for doubt that the location of the activating computers was unknown and that the purpose of deploying the NIT was to aid in identifying their location. Among other things, the affiant explained that without the use of the NIT, "the identities of the administrators and users of [Playpen] would remain unknown." Def.'s Ex. B ¶ 29; *see also* Def.'s Ex. B ¶ 32 ("[U]sing a NIT may help FBI agents locate the administrators and users" of Playpen.); Def.'s Ex. B ¶ 31 (noting the NIT was a "presently available investigative technique with a reasonable likelihood of securing the

evidence necessary to prove . . . the actual location and identity" of Playpen users "engaging in the federal offenses enumerated."). And, the affiant specifically requested authority for the NIT to "cause an activating computer—wherever located—to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." Def.'s Ex. B ¶ 46(a).

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of Playpen that would be downloaded through normal operation of the site. Def.'s Ex. B ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. Def.'s Ex. B ¶ 33. The affidavit specifically requested authority to deploy the NIT to any user who logged into Playpen with a username and a password. Def.'s Ex. B ¶ 36.

As other courts have found, the only fair reading of the NIT warrant, application, affidavit, and attachments leads to one conclusion: the government sought authority to deploy the NIT to any computer that entered the Eastern District of Virginia and logged into Playpen, regardless of the physical location of that computer. *See e.g.*, *Michaud*, 2016 WL 337263, at *3-4 (rejecting defendant's assertion that deploying the NIT to a computer outside of the Eastern District of Virginia exceeded the scope of the NIT Warrant's authorization). Owens's self-serving insistence that the Court confine its inquiry to text

in the face sheet of the warrant is understandable but unsupportable. And it certainly does not justify suppression.

E. None of Owens's claimed defects in the NIT warrant justify the extraordinary remedy of suppression and, even if that warrant does not satisfy the Fourth Amendment, the good faith exception bars suppression.

As a threshold matter, Owens's dissatisfaction with having been discovered through the NIT is understandable. But the mere fact that he objects to having been unmasked, without more, does not justify suppression of evidence obtained pursuant to a warrant issued by a neutral and detached magistrate judge based on a finding of probable cause. For all of the reasons outlined above, the NIT warrant does not contravene the requirements of the Fourth Amendment. But even if it did somehow do so, suppression of the information derived from the execution of that warrant is not appropriate.

The Fourth Amendment's exclusionary rule does not provide "a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search." *Davis v. United States*, 564 U.S. 229, 236 (2011) (quoting *Stone v. Powell*, 428 U.S. 465, 468 (1976)) (internal quotation marks omitted). The exclusionary "rule's sole purpose . . . is to deter future Fourth Amendment violations." *Id.* at 236-37 (collecting cases). The real deterrent value "is a 'necessary condition for exclusion,' but it is not a 'sufficient' one." *Id.* at 237 (quoting *Hudson v. Michigan*, 547 U.S. 586, 596 (2006)). There are substantial costs associated with its application. *Id.* ("Exclusion exacts a heavy toll on both the judicial system and society at large. . . . It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence."). The practical

effect in nearly every case "is to suppress the truth and set the criminal loose in the community without punishment." *Id.* (citing *Herring v. United States*, 555 U.S. 135, 141 (2009)). Accordingly, it is to be employed "only as a 'last resort'"—that is, when "the deterrence benefits of suppression . . . outweigh its heavy costs." *Id.* (quoting *Hudson*, 547 U.S. at 591).

Under the good faith exception to the Fourth Amendment's exclusionary rule, suppression is not warranted when officers rely in good faith on an objectively reasonable search warrant issued by a neutral and detached judge. *United States v. Leon*, 468 U.S. 897, 900 (1984). This objective standard is measured by "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922 n.23. "[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Id.* at 922 (internal quotation marks omitted). The Supreme Court observed that "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Id.* at 918. The Court identified only four circumstances in which exclusion of evidence seized pursuant to a warrant is appropriate. Those are when: (1) the issuing magistrate was misled by the inclusion of knowing or recklessly false information; (2) the issuing magistrate wholly abandoned the detached and neutral judicial role; (3) the warrant is facially deficient as to its description of the place to be searched or the things to be seized; or (4) the affidavit upon which the

warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely on it in good faith. *Id.* at 923-924. None apply here.

Here, the NIT warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. Nor does the defendant allege that the issuing magistrate judge abandoned her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. And the affidavit made a strong, comprehensive showing of probable cause to deploy the NIT. Once the magistrate judge signed the warrant, having been made aware of how the NIT would be implemented and its reach, the agents' reliance on that authority was objectively reasonable. *See Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested."). Ultimately, agents acted reasonably in relying on the magistrate's authorization of the NIT warrant, and so the evidence seized pursuant to it should not be suppressed. *See e.g.*, *Michaud*, 2016 WL 337263, at *7 ("Because reliance on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted."); *Matish*, 2016 WL 3545776, at *25 ("The agents' reliance on the NIT Warrant was objectively reasonable, and it appears to the Court that the agents acted in good faith.").

IV. Conclusion

For the foregoing reasons, the United States respectfully requests that Owens's Motion to Suppress be denied.

Dated at Milwaukee, Wisconsin this 15th day of August, 2016.

Respectfully submitted,

GREGORY J. HAANSTAD
United States Attorney

By s/

BENJAMIN W. PROCTOR
Assistant United States Attorney
Benjamin Proctor Bar No.: 1051904
Attorney for Plaintiff
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Ave. Suite 530
Milwaukee, Wisconsin 53202
Tel: (414) 297-1700
Email: benjamin.proctor@usdoj.gov